Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1.-51. (Cancelled).

52. (New) An apparatus, comprising:

an inbound IPSec packet processing path, comprising:

i) inbound network interface logic circuitry to present an inbound IPSec packet to said inbound IPSec packet processing path after said inbound IPSec packet has been received at said apparatus;

ii) inbound IPSec decryption logic circuitry to perform IPSec decryption processing on said inbound IPSec packet if said inbound IPSec packet warrants said IPSec decryption processing;

iii) a first region of memory coupled to said inbound IPSec decryption logic circuitry, said first region of memory to store security policy information that indicates whether or not said inbound IPSec packet warrants said IPSec decryption processing;

iv) a second region of memory coupled to said inbound IPSec decryption logic circuitry, said second region of memory to store IPSec security association information that indicates what said IPSec decryption processing entails;

v) inbound DMA controller logic circuitry to place said inbound IPSec packet into an offload memory, said offload memory not being a memory where instructions

and data evicted from said apparatus's Central Processing Unit's cache are initially stored;

vi) a first inbound buffer coupled between said inbound network interface logic circuitry and said inbound IPSec decryption logic, said first buffer to hold said inbound IPSec packet before it is presented to said inbound IPSec decryption logic circuitry;

vii) a second inbound buffer coupled between said inbound IPSec decryption logic circuitry and said inbound DMA controller, said second inbound buffer to present said inbound IPSec packet to said DMA controller; and,

viii) a first path from said first inbound buffer to said second inbound buffer that flows through said IPSec decryption logic circuitry, a second path from said first inbound buffer to said second inbound buffer that does not flow through said IPSec decryption logic circuitry, said inbound IPSec packet to flow along said first path if said security policy information indicates that said inbound IPSec packet warrants said IPSec decryption processing, said inbound IPSec packet to flow along said second path if said security policy information indicates that said inbound IPSec packet does not warrant said IPSec decryption processing.

53. (New) The apparatus of claim 52 further comprising:

an outbound IPSec packet processing path, comprising:

i) outbound network interface logic circuitry to accept an outbound IPSec packet from said outbound IPSec packet processing path before said outbound IPSec packet is transmitted from said apparatus;

ii) outbound IPSec encryption logic circuitry to perform IPSec encryption processing on said outbound IPSec packet if said outbound IPSec packet warrants said IPSec encryption processing;

iii) a third region of memory coupled to said outbound IPSec encryption logic circuitry, said third region of memory to store outbound security policy information that indicates whether or not said outbound IPSec packet warrants said IPSec encryption processing;

iv) a fourth region of memory coupled to said outbound IPSec encryption logic circuitry, said fourth region of memory to store IPSec security association information that indicates what said IPSec encryption processing entails;

v) outbound DMA controller logic circuitry to fetch said outbound IPSec packet from said offload memory;

vi) a first outbound buffer coupled between said outbound DMA controller and said outbound IPSec encryption logic circuitry, said first outbound buffer to present said outbound IPSec packet to said IPSec encryption logic circuitry;

vii) a second outbound buffer coupled between outbound IPSec encryption logic and said outbound network interface logic circuitry, said second buffer to hold said outbound IPSec packet before it is presented to said outbound network interface logic circuitry; and,

viii) a third path from said first outbound buffer to said second outbound buffer that flows through said IPSec encryption logic circuitry, a fourth path from said first outbound buffer to said second outbound buffer that does not flow through said IPSec encryption logic circuitry, said outbound IPSec packet to flow along

said third path if said outbound security policy information indicates that said outbound IPSec packet warrants said IPSec encryption processing, said outbound IPSec packet to flow along said second path if said outbound security policy information indicates that said outbound IPSec packet does not warrant said IPSec encryption processing.

54. (New) The apparatus of claim 53 wherein said inbound network interface logic circuitry comprises inbound Ethernet network interface logic circuitry and said outbound network interface logic circuitry comprises outbound Ethernet network interface logic circuitry.

55. (New) The apparatus of claim 52 wherein said inbound network interface logic circuitry comprises inbound Ethernet network interface logic circuitry and said outbound network interface logic circuitry comprises outbound Ethernet network interface logic circuitry.